Int. J. on Recent Trends in Engineering and Technology, Vol. 8, No. 1, Jan 2013

A Generalized Image Authentication Based On Statistical Moments of Color Histogram

Dattatherya[1], S. Venkata Chalam[2], Manoj Kumar Singh[3]
[1](Department of TCE/Dyananda Sagar College of Engineering, Bangalore, 500078, India)
[2](Department of ECE/ CVR College of Engineering, Hyderabad, 501510, India)
[3](Director/Manuro Tech Research/Bangalore, 560097, India)
Email: [1]dattugujjar28@yahoo.com, [2]sv_chalam2003@yahoo.com,[3]mksingh@manuroresearch.com

***Abstract*— Designing low cost and high speed authentication solution for digital images is always an attractive area of research in image processing. In past few years because of widespread use of internet and network technology, concept of information distribution has been become habit rather than exception in daily life. In same aspects challenges involved with distribution of authenticate information has been increased manifolds. In this paper a generalize image authentication method has proposed by hybridization of color histogram and associated first four statistical moments to achieve the objectives of low cost and high speed. Proposed method can apply for both gray and color images having any size and any format. Solution generates a very small authentication code with an ease means which is use to analyze the characteristics of received image from tampering perspective.**

***Index Terms*— image authentication, histogram, statistical moments, Skewness, Kurtosis**.

I. Introduction

The changes in images may be intentionally malicious or may inadvertent affect the interpretation of the work. For example, an inadvertent change to an X-ray image might result in a misdiagnosis, where as malicious tampering of photographic evidence in a criminal trial can result in either wrong convection or acquittal. Thus, in applications for which we must be certain a work has not been altered, there is as need for verification or authentication of the integrity of the content. Authenticity, by definition, means something as being in accordance with fact, as being true in substance", or as being what it professes in origin or authorship, or as being genuine." A third definition of authenticity is to prove that something is actually coming from the alleged source or origin." For instance, in the courtroom, insurance company, hospital, newspaper, magazine, or television news, when we watch/hear a clip of multimedia data, we hope to know whether the image/video/audio is authentic. For electronic commerce, once a buyer purchases multimedia data from the Internet, she needs to know whether it comes from the alleged producer and she must be assured that no one has tampered with the content. The credibility of multimedia data is expected for the purpose of being electronic evidence or a certified product. In practice, different requirements affect the methodologies and designs of possible solutions. In contrast with traditional sources whose authenticity can be established from many physical clues, multimedia data in electronic forms (digital or analog) can only be authenticated by non-physical clues. However, multimedia data are usually distributed and re-interpreted by many interim entities (e.g., editors, agents). Because of this, it becomes important to guarantee end-to-end trustworthiness between the origin source and the final recipient. That can be achieved by the robust digital signature method that .Although the "word authentication" has three broad meanings: the integrity of data, the alleged source of data, and the reality of data. We use the word "copyright protection" to indicate the second meaning: alleged source. The third meaning, the reality of data, may be addressed by using a mechanism linking the information of alleged source to real world capturing apparatus such as a digital camera.

Watermarking has been considered to be a promising solution that can protect the copyright of multimedia data through transcoding, because the embedded message is always included in the data. However, today, there is no evidence that watermarking techniques can achieve the ultimate goal to retrieve the right owner information from the received data after all kinds of content-preserving manipulations.Watermarking is distinguished from other techniques in three important ways. First, watermarks are imperceptible. Unlike bar codes, they do not detract from the aesthetics of an image. Second, watermarks are inseparable from works in which they are embedded. Unlike header fields, they do not get removed when the works are displaced or converted to other file formats. Finally, watermarks undergo the same transformation as the works. The potential benefits of avoiding any separate store and subtle must be weighted against added Complexity of using a watermark for authentication rather than other approaches. Furthermore there is a potentially serious adverse side effect of watermarking; embedding a watermark changes a work, albeit in a known and controlled manner. If we want to verify that works are not changed, some applications may find even imperceptible alterations unacceptable. It is these attributes that make watermarking invaluable for certain applications. Because of the fidelity constraint, watermarks can only be embedded in a limited space in the multimedia data. There is always a biased advantage for the attacker whose target is only to get rid of the watermarks by exploiting various manipulations in the finite watermarking embedding space.In section II related works where as in section III description of histogram and definition of various moments are given. Physical interpretations of these moments are discussed in section IV. Architecture of design solution and experimental

DOI: 01.IJRTET.8.1.32

analysis has presented in section V. Conclusion and references have given at the end.

II. Related Work

In [1] authors introduced a digital-signature approach to content-based image authentication based on unit-linking PCNN (pulse coupled neural network), which consists of spiking neurons and has biological support. In this method, local image icon produced by unit-linking PCNN as image feature. Authors of [2] have image authentication scheme based on cell neural network with hyper-chaos characteristics (HCCNN). In the scheme, the authentication code, which is used as secret key and the pixel values of image are used for the input of HCCNN. The secret information that HCCNN produces is transmitted to the receiving end through secret channel. The receiver can then use the received secret information to authenticate the suspect image by comparing the original authentication code with that calculated from the suspect image. Article in [3] proposes a palette-based color image authentication mechanism. Morphological operations are adopted to draw out the tampered area precisely. Authors in [4] propose an image authentication scheme which detects illegal modifications for image vector quantization (VQ).

In the proposed scheme, the index table is divided into non-overlapping index blocks. The authentication data is generated by using the pseudo random sequence. image authentication which can prevent malicious manipulations but allow JPEG lossy compression. The authentication signature is based on the invariance of the relationships between discrete cosine transform (DCT) coefficients at the same position in separate blocks of an image. These relationships are preserved when DCT coefficients are quantized in JPEG compression in [5].In [6],authors have proposed a method by dividing the image into blocks in a multilevel hierarchy and calculating block signatures in this hierarchy. While signatures of small blocks on the lowest level of the hierarchy ensure superior accuracy of tamper localization, higher level block signatures provide increasing resistance to VQ attacks. At the top level, a signature calculated using the whole image completely thwarts the counterfeiting attack. [7] Presented an approach using distributed source coding for image authentication. The key idea is to provide a Slepian-Wolf encoded quantized image projection as authentication data. This version can be correctly decoded with the help of an authentic image as side information. Distributed source coding provides the desired robustness against legitimate variations while detecting illegitimate modification. The decoder incorporating expectation maximization algorithms can authenticate images which have undergone contrast, brightness, and affine warping adjustments. Digital image anti-tampering authentication scheme based on semi-fragile watermarking algorithm is given. The system implements two modes of embedding for single image and batch image has presented in [8].In [9] an erasable watermark is embedded in each block of a document image independently for secure localization is presented. The embedding process introduces some background noise; however the content in the document can be read or understood by the user, because human vision has the inherent capability to recognize various patterns in the presence of noise. After verifying the content of each block, the exact copy of original image can be restored at the blind detector for further analysis. In [10] authors have investigated existing image hash algorithms, and design an novel image hash based on human being's visual system. In this algorithm, they capture the perceptual characters of the image using Gabor filter which can sense the directions in the image just like human's primary visual cortex. For a given image, they have compute the reference scale, direction and block to make sure the final hash can resist against rotation, scale, and translation attacks while maintain the sensitivity to local malicious manipulations. Authors in [11] based on artificial neural network have presented the concept of authentication where various objectives like compression, security, authentication and localization have unified.

III. Utilised Statistical Parameters

A. Color Histogram

This is most commonly used color feature in image processing. Color histogram has been found to be very effective in characterizing the global distribution of colors in an image, and it can be used as an important feature for image characterization. To define color histogram, the color space is quantized into a finite number of discrete levels. Each of these levels becomes a bin in the histogram. The color histogram is then computed by counting the number of pixels in each of these discrete levels. Histogram for a specific image carries entire tonal distribution of that particular image.

B. Color Moment

This is compact representation of color feature to characterize a color image. It is possible that most of the color distribution information is captured by the four low order moments. The first order moment (μ_c) captures the mean color, the second order moment (σ_c) captures the standard deviation, third order moment captures the skewness (θ_c) and fourth order moment (β_c) captures the kurtosis of the color distribution. These four low order moments $(\mu_c, \sigma_c, \theta_c, \beta_c)$ are extracted for each of the three color planes using the following mathematical formulation.

$$\mu_c = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} p_{ij}^{c} \qquad (1)$$

$$\sigma_c = \left[\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(p_{ij}^{c} - \mu_c\right)^2\right]^{\frac{1}{2}} \qquad (2)$$

DOI: 01.IJRTET.8.1.32

$$\theta_c = \left[\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(p_{ij}^{c} - \mu_c \right)^3 \right]^{\frac{1}{3}} \quad (3)$$

$$\beta_c = \left[\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(p_{ij}^{c} - \mu_c \right)^4 \right]^{\frac{1}{4}} \quad (4)$$

IV. Physical Significance of First Four Moments

A. First Order Moment: Mean (Measures of Central Tendency)

A frequency distribution, in general shows clustering of the data around some central value. Finding of this central value or the average is of importance as it gives a most representative value of the whole group.

B. Second Order Moment: Standard Deviation (Measure of Dispersion)

Although measure of central tendency do exhibit one of the important characteristics of a distribution, they fail to give any idea as to how the individual values differ from the central value,i.e. whether they are closely packed around the central value or widely scattered away from it.

C. Third Order Moment: Skewness (Measure Degree of Asymmetry)

The skewness value can be positive or negative, or even undefined. Qualitatively, a negative skew indicates that the tail on the left side of the probability density function is longer than the right side and the bulk of the values (possibly including the median) lie to the right of the mean. A positive skew indicates that the tail on the right side is longer than the left side and the bulk of the values lie to the left of the mean. A zero value indicates that the values are relatively evenly distributed on both sides of the mean, typically but not necessarily implying a symmetric distribution .If skewness is positive, the data are positively skewed or skewed right, meaning that the right tail of the distribution is longer than

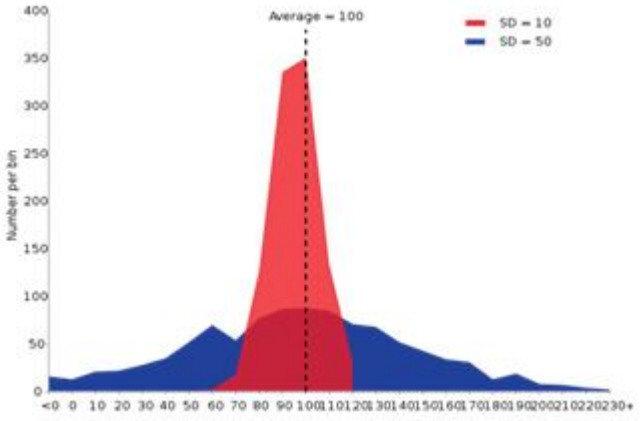


Fig. 1. Example of two sample populations with the same mean and different standard deviations. Red population has mean 100 and SD 10; blue population has mean 100 and SD 50.

the left. If skewness is negative, the data are negatively skewed or skewed left, meaning that the left tail is longer.If skewness = 0, the data are perfectly symmetrical. But a skewness of exactly zero is quite unlikely for real-world data, so how can interpret the skewness number?

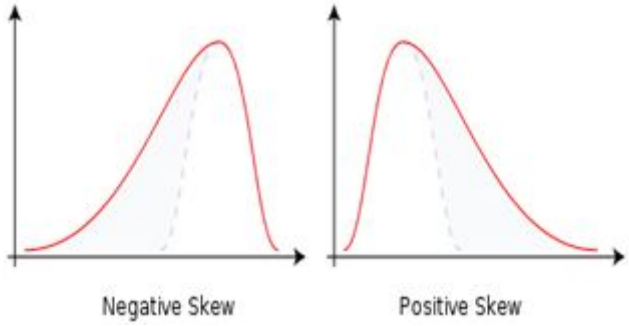


Fig. 2. Different types of skewness.

- If skewness is less than "1 or greater than +1, the distribution is highly skewed.
- If skewness is between "1 and "½ or between +½ and +1, the distribution is moderately skewed.
- If skewness is between "½ and +½, the distribution is approximately symmetric.

D. Forth Order Moment: Kurtosis (Measure the Degree of Peakedness)

Statistics distributions can be characterized in terms of central tendency, variability, and shape. With respect to shape, virtually skewness is used, on the other hand, another aspect of shape, which is kurtosis. Kurtosis is frequently not reported in research articles, in spite of the fact that virtually every statistical package provides a measure of kurtosis. This occurs most likely because kurtosis is not well understood and because the role of kurtosis in various aspects of statistical analysis is not widely recognized. If a distribution is given, the next question is about the central peak: is it high and sharp, or short and broad? We can get some idea of this from the histogram, but a numerical measure is more precise. The height and sharpness of the peak relative to the rest of the data are measured by a number called kurtosis.

Higher values indicate a higher, sharper peak; lower values indicate a lower, less distinct peak. This occurs because; higher kurtosis means more of the variability is due to a few extreme differences from the mean, rather than a lot of modest differences from the mean. Same thing in another way: increasing kurtosis is associated with the "movement of probability mass from the shoulders of a distribution into its center and tails". The reference standard is a normal distribution, which has a kurtosis of 3. In token of this, often the excess kurtosis is presented: excess kurtosis is simply kurtosis 3.A normal distribution has kurtosis exactly 3 (excess kurtosis exactly 0). Any distribution with kurtosis ≈3 (excess ≈0) is called "mesokurtic".A distribution with kurtosis <3 (excess kurtosis <0) is called "platykurtic". Compared to a normal distribution, its central peak is lower and broader, and its tails are shorter and thinner. A distribution with kurtosis >3 (excess kurtosis >0) is called "leptokurtic".

DOI: 01.IJRTET.8.1.32

Compared to a normal distribution, its central peak is higher and sharper, and its tails are longer and fatter.

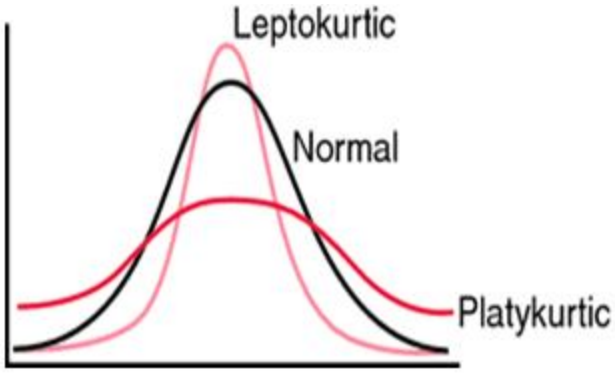


Fig. 3. Different Types of kurtosis

V. Architecture and Experiments of the Proposed Scheme

The proposed image content authentication scheme is shown in Fig.4. Here, the image matrix data applied to find the color histogram. Depending upon grayscale or color image there are either one histogram or three set of histogram each one corresponding to red, green and blue color respectively. These histograms capture the distribution of pixels over the image and defined a kind of distribution. Characteristics of histogram distribution can be captured by getting its first four statistical moments and these are mean, standard deviation, skewness and kurtosis. Each and every parameter captures the unique feature available under the particular histogram distribution curve. These parameters form the authentication code for that particular image .length of code is equal to 3 or 12 depends upon the gray or color image. This original code transmitted through the secret channel and image through public channel to the receiver side. During distribution, media data may be tampered maliciously at the receiver side with the received image an authentication code from histogram and first four moments generated as it done at transmitting side. A comparison is made between both authentication codes and a relative Euclidian distance measure defined to decide the tampering occurrence and level of that.

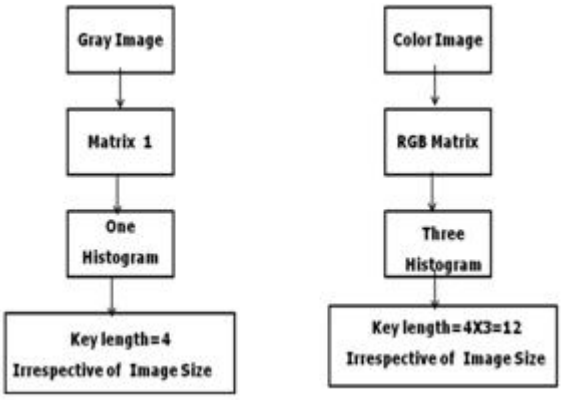


Fig. 4. Block Diagram for Key Generation

With the proposed concept of authentication, various color images and grayscale images are taken for experiments. There is no preprocessing of image is required which further save the time of total execution process. In the test case 1, a color image is taken as shown in Fig.6. its three histogram and corresponding first four moments are calculated by (1) to (4) as shown in table 1.intentionally tampering has given off line over this image as shown in Fig.6(c) where a green horizontal bar(by making red color pixels equal to zero) is placed over the original image. With this tampered image histograms are shown in Fig.6(d) and corresponding authentication key has shown in table 2.the difference in the statistical parameter is very clearly observed. To have the understanding of tampering level normalized differences have plotted in Fig.6(e) and a relative normalized Euclidian distance (RNED) has obtained by (5). To see the more clear understanding gray scale image test case has also taken and performances have shown in Fig.7.

$$RNED = \sqrt{\sum_{i=1}^{n}\left(\left|\left(\left|\frac{RAC}{TAC}\right|-1\right)\right|\right)^2} \qquad (5)$$

Where RAC and TAC represent the authentication code generated at the receiver and transmitter side.

Conclusion

Requirement of having the very efficient method which could handle the problem of image authentication has proposed in this paper. Focus has given to make the solution very cost effective and with high processing speed with simple concept of statistical characteristics of image data. Developed method is applicable to any size and any type without variation in solution complexity. It is also observed that skewness and kurtosis are more sensitive parameters in terms of authentication. The proposed method has developed to keep the things in mind the there are number of applications where more important part is authentication of image rather than tampering localization and reconstruction of tampered location.

References

[1] Xiaodong Gu ,"A New Approach to Image Authentication using Local Image Icon of Unit-linking PCNN",Neural Networks, 2006. IJCNN '06. page(s): 1036 - 1041 .

[2] Gao,Gu,Emmanuel," A novel image authentication scheme based onhyper-chaotic cell neural network", Chaos, Solitons & Fractals,Volume 42, Issue 1, 15 October 2009, Pages 548–553,Elsevier

[3] Chang, Pei-Yu-Lin,"A Color Image Authentication Method Using Partitioned Palette and Morphological Operations",IEICE,VolumeE91-D Issue1,January 2008,page:54-61,Oxford university press,Oxforrd UK

[4] Jun-Chou Chuang, Yu-Chen Hu," An adaptive imageauthentication scheme for vector quantization compressed image"Journal of Visual Communication and Image Representation,Volume 22, Issue 5, July 2011, Pages 440–449,Elsevier.

[5] Shih-Fu Chang,"A robust image authentication method distinguishing JPEG compression from malicious manipulation",Circuits and Systems for Video Technology,

DOI: 01.IJRTET.8.1.32

IEEE Transactions on, Feb 2001,Volume: 11 , Issue: 2 Page(s): 153 – 168.

[6] Utku Celik, M.," Hierarchical watermarking for secure image authentication with localization",Image Processing, IEEE Transactions on,Jun 2002,Volume: 11 , Issue: 6 ,Page(s): 585 – 595

[7] Yao-Chung Lin ,"Image Authentication Using Distributed Source Coding",Image Processing, IEEE Transactions on, Jan. 2012,Volume: 21 , Issue: 1 ,Page(s): 273 – 283.

[8] "A Tamper-Resistant Authentication Scheme on Digital Image",Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering ,Advances in Intelligent Systems and Computing Volume 181, 2013, pp 867-872 ,springer

[9] Niladri B. Puhan, A.T.S.Ho ," Secure Tamper Localization in Binary Document Image Authentication",Knowledge-Based Intelligent Information and Engineering Systems ,LNCS,Volume 3684, 2005, pp 263-271 ,springer.

[10] Wang,jiang,lian,hu," Image authentication based on perceptual hash using Gabor filters", Soft Computing ,March 2011, Volume 15, Issue 3, pp 493-504 ,springer.

[11] Dattatherya, Chalam & Singh," Unified approach with neural network for authentication, security and compression of image: UNICAP" (IJIP), Volume (6) : Issue (1) : 2012,PP:13-25.

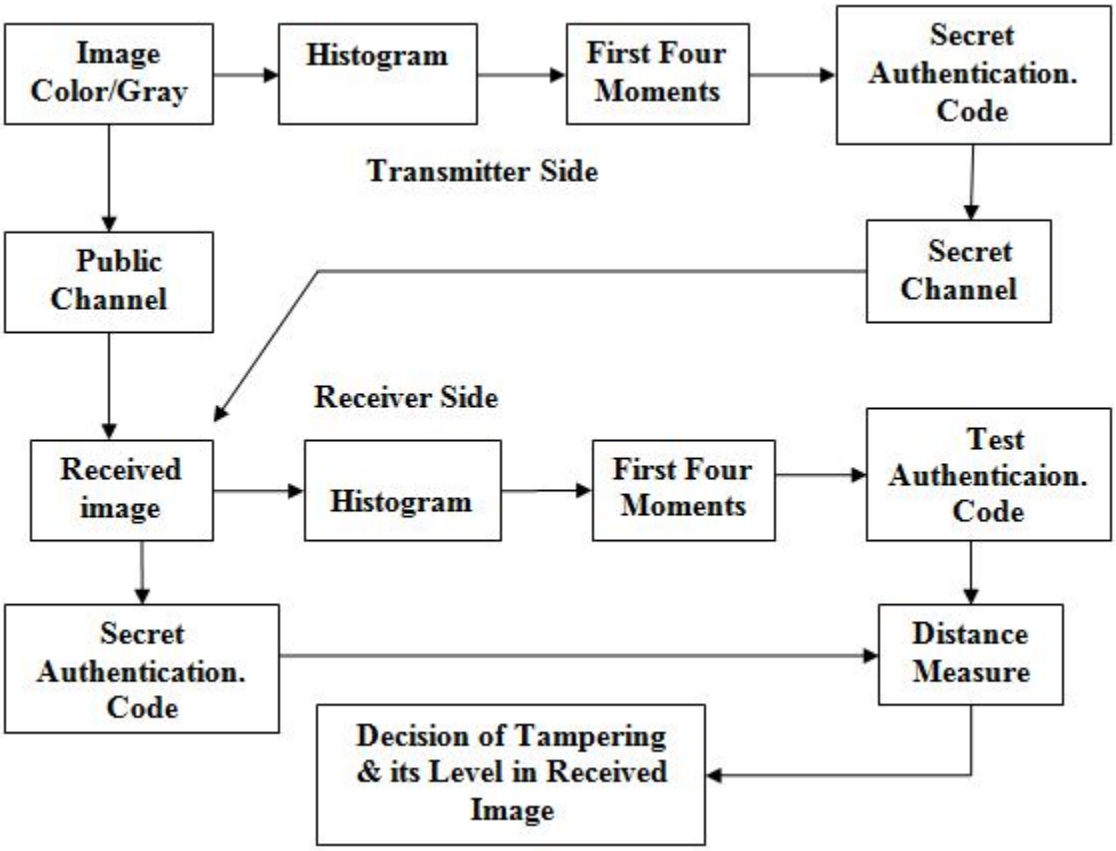


Fig. 4. Proposed architecture for image authentication

Test case 1: Image Size -1280 × 960 × 3

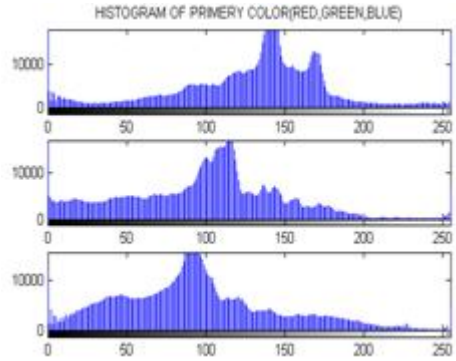
Transmitter side operation

(a)

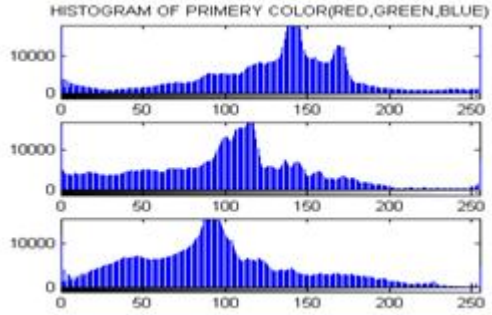
Receiver side operation

(c)

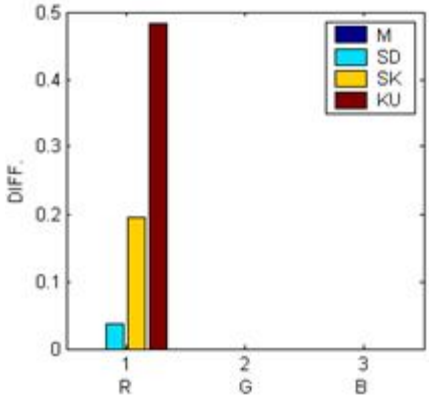
DOI: 01.IJRTET.8.1.32



(b)



(d)



(e)

Fig. 6. Proposed architecture performance for a color image, tampering has given at the receiver side.

TABLE I. STATISTICAL MOMENTS (MEAN, STANDARD DEVIATION, SKEWNESS AND KURTOSIS) OF TRANSMITTED AUTHENTICATION CODE FOR COLOR IMAGE.

Transmitted Authentication Code			
Moments	**Red**	**Green**	**Blue**
(μ_c)	4800	4800	4800
(σ_c)	5413.9	4821.8	3974.7
(θ_c)	2.3941	3.8551	1.3936
(β_c)	9.8566	31.3629	4.9738

TABLE II. STATISTICAL MOMENTS (MEAN, STANDARD DEVIATION, SKEWNESS AND KURTOSIS) OF TEST AUTHENTICATED CODE FOR COLOR IMAGE.

Test Authenticated Code			
Moments	**Red**	**Green**	**Blue**
(μ_c)	4800	4800	4800
(σ_c)	**5611.5**	4821.8	3974.7
(θ_c)	**2.8587**	3.8551	1.3936
(β_c)	**14.6169**	31.3629	4.9738
Level of tampering with Relative Euclidean distance = 0.4242			

Test case 2: Image Size -512×512

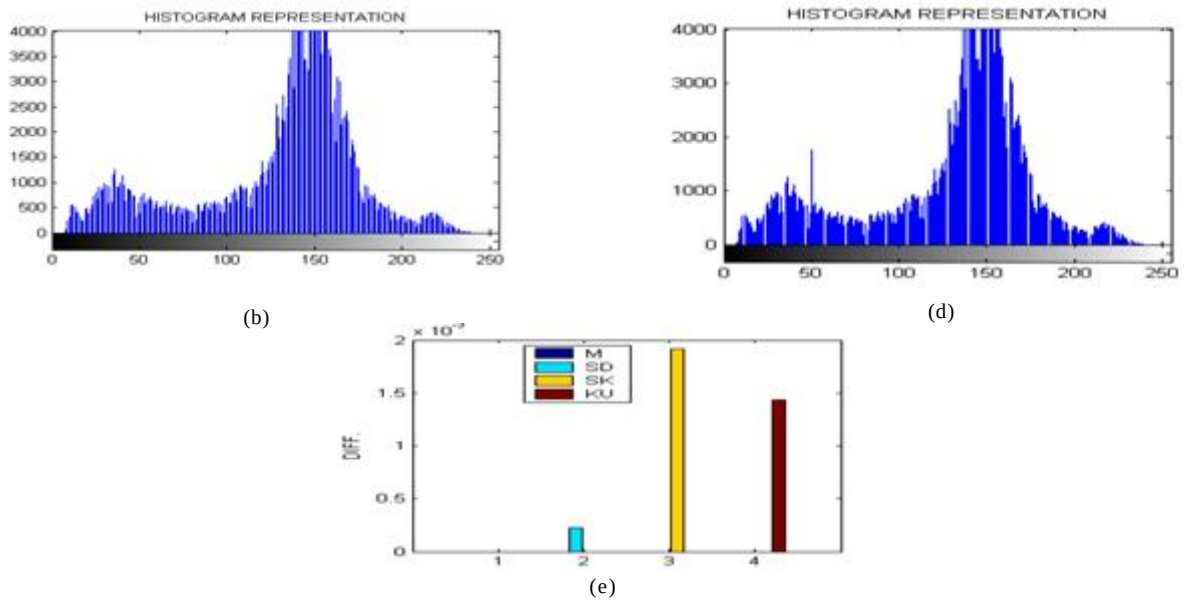
Transmitter side operation

Receiver side operation

(a)

(c)

DOI: 01.IJRTET.8.1.32



(b) (d)

(e)

Fig. 7. Proposed architecture performance for a gray scale image, tampering has given at the receiver side

TABLE III. STATISTICAL MOMENTS (MEAN, STANDARD DEVIATION, SKEWNESS AND KURTOSIS) OF TRANSMITTED AUTHENTICATION CODE FOR GRAYSCALE IMAGE.

Transmitted Authentication Code	
Moments	
(μ_c)	1024
(σ_c)	1241.7
(θ_c)	2.0346
(β_c)	6.5052

TABLE IV. STATISTICAL MOMENTS (MEAN, STANDARD DEVIATION, SKEWNESS AND KURTOSIS) OF TEST AUTHENTICATED CODE FOR GRAYSCALE IMAGE.

Test Authenticated Code	
Moments	
(μ_c)	1024
(σ_c)	1241.5
(θ_c)	2.0307
(β_c)	6.4958
Level of tampering with Relative Euclidean distance = 0.0035	

DOI: 01.IJRTET.8.1.32